学校编码：10384　　分类号____密级_____

学　　号：23320141153252　　UDC_____

厦门大学

硕 士 学 位 论 文

基于多监督点的无线物理层认证方法研究

Study on Physical-Layer Authentication with Multiple Landmarks in Wireless Networks

李 强 达

指导教师姓名： 肖 亮 教授

专 业 名 称： 电子与通信工程

论文提交日期： 2017 年 月

论文答辩时间： 2017 年 月

学位授予日期： 2017 年 月

答辩委员会主席：_____

评 阅 人：_____

2017 年 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“ √ ”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

随着移动互联网和物联网等的发展，无线网络由于开放性和移动性，受到严峻的安全挑战。电子欺骗攻击者伪造其他用户的身份信息，发送具有虚假媒体接入控制地址的数据包，旨在获取非法用户权限，甚至通过攻击控制信道达到拒绝服务攻击。物理层认证技术利用物理层特征，例如信道响应随发射机位置而改变的特性检测电子欺骗者，认证开销小，但是认证精度有待提高。

论文采用多天线技术和多监督节点，构建分布式认证网络，增加认证的信道信息来源，显著提高认证的准确率。该系统采用逻辑回归模型，不依赖于特定的无线信道模型，具有更强的普适性。在此基础上，论文提出基于 Frank-Wolfe 算法的集中式认证方案。

针对该分布式网络，论文设计基于 DFW(Distributed Frank-Wolfe)的分布式认证算法，提出分布式认证方案，降低多监督节点之间的通信量。仿真结果表明，该方案不但可以保证 Frank-Wolfe 算法的检测精度，而且显著降低每次认证的通信量。例如，针对 8 个配备 8 个接收天线的监督节点所组成的认证网络，所提算法相比基于 Frank-Wolfe 的认证方案减少了 28.9%的通信量，其检测电子欺骗的误警率低于 2%和漏报率低于 0.1%。

为了减轻基于 DFW 的认证方案对有标签训练数据的依赖，同时降低认证系统通信量，论文采用用户信道信息建立用户身份文档，提出基于分布式学习算法 DK-Means(Distributed K-Means)的无线物理层认证方案。仿真结果表明，所提方案在降低系统通信量的同时，提高了认证系统的认证准确率，能够抵御移动电子欺骗攻击。例如在监督节点个数为 8 的时候，所提算法相比基于 DFW 的认证方案减少了 51.6%的通信量，达到了 99.9%的认证准确率。

关键字：物理层安全；认证；机器学习；

Abstract

With the development of mobile Internet and Internet of Things (IoT), wireless network is threatened by attackers because of its open and mobile characteristics. The spoofing attacker with faked Media Access Control (MAC) address sends spoofing packets to obtain illegal advantages and further perform denial-of-service attacks. Physical (PHY)-layer authentication techniques exploit physical layer properties of wireless communications, such as the channel responses that varies with position to detect spoofing attacks. Although PHY-layer authentication scheme has less computation costs, the detection accuracy has to be improved.

In this paper, a distributed authentication network based on Multiple-input Multiple-output (MIMO) technique and multiple landmarks is proposed to improve the authentication accuracy with sufficient user channel information. The authentication model based on the logistic regression does not relay on specific channel model, and has a general validity. On this basis, a centralized authentication scheme based on Frank-Wolfe algorithm is proposed.

A distributed authentication scheme based on distributed Frank-Wolfe (DFW) algorithm is further proposed for the distributed authentication network to reduce the communication cost among landmarks. The experiment results show that the proposed authentication scheme can reduce the communication cost with high detection accuracy. For example, compared with the scheme based on Frank-Wolfe, the proposed scheme with 8 landmarks and 8 antennas reduces the communication cost by 28.9% with 2% false alarm rate and 0.1% miss detection rate.

With user's identity document based on channel information, a distributed

authentication scheme based on Distributed K-Means (DK-Means) algorithm is proposed to reduce the dependency on the labeled training data in DFW based authentication scheme, and further reduce the communication cost. The experiment results show that the proposed scheme reduces the communication cost with high spoofing detection accuracy. For example, compared with the DFW based authentication scheme, the proposed scheme with 8 landmarks decreases the communication cost by 51.6% with 99.9% authentication accuracy.

Key Words: PHY-layer security; Authentication; Machine learning

目 录

Contents

常用符号表

符号	含义
M	监督节点个数
N	监督节点天线数
J	攻击用户数
H_m^i	监督节点 m 上数据包 i 的信道信息
$\mathbf{H}_i$	数据包 i 的系统信道信息向量
y_i	数据包 i 的认证结果
β_0	认证模型截距
$\boldsymbol{\beta}$	认证模型参数
P_f	系统误警率
P_m	系统漏报率
G_{Alice}	用户 Alice 的身份文档
G_{Eve}	用户 Eve 的身份文档
ATR	平均认证准确率
AFR	平均认证错误率